AOM-TPM-9655V
AOM-TPM-9655H

USER'S MANUAL

Revision 1.0

The information in this User's Manual has been carefully reviewed and is believed to be accurate. The vendor assumes no responsibility for any inaccuracies that may be contained in this document, and makes no commitment to update or to keep current the information in this manual, or to notify any person or organization of the updates. **Please Note: For the most up-to-date version of this manual, please see our web site at www.supermicro.com.**

Super Micro Computer, Inc. ("Supermicro") reserves the right to make changes to the product described in this manual at any time and without notice. This product, including software and documentation, is the property of Supermicro and/or its licensors, and is supplied only under a license. Any use or reproduction of this product is not allowed, except as expressly permitted by the terms of said license.

IN NO EVENT WILL Super Micro Computer, Inc. BE LIABLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, SPECULATIVE OR CONSEQUENTIAL DAMAGES ARISING FROM THE USE OR INABILITY TO USE THIS PRODUCT OR DOCUMENTATION, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN PARTICULAR, SUPER MICRO COMPUTER, INC. SHALL NOT HAVE LIABILITY FOR ANY HARDWARE, SOFTWARE, OR DATA STORED OR USED WITH THE PRODUCT, INCLUDING THE COSTS OF REPAIRING, REPLACING, INTEGRATING, INSTALLING OR RECOVERING SUCH HARDWARE, SOFTWARE, OR DATA.

Any disputes arising between manufacturer and customer shall be governed by the laws of Santa Clara County in the State of California, USA. The State of California, County of Santa Clara shall be the exclusive venue for the resolution of any such disputes. Supermicro's total liability for all claims will not exceed the price paid for the hardware product.

FCC Statement: Refer to Supermicro's web site for FCC Compliance Information.

California Best Management Practices Regulations for Perchlorate Materials: This Perchlorate warning applies only to products containing CR (Manganese Dioxide) Lithium coin cells. "Perchlorate Material-special handling may apply. See www.dtsc.ca.gov/hazardouswaste/perchlorate".

WARNING: Handling of lead solder materials used in this product may expose you to lead, a chemical known to the State of California to cause birth defects and other reproductive harm.

Manual Revision 1.0

Release Date: March 13, 2014

Unless you request and receive written permission from Super Micro Computer, Inc., you may not copy any part of this document.

Information in this document is subject to change without notice. Other products and companies referred to herein are trademarks or registered trademarks of their respective companies or mark holders.

Copyright © 2014 by Super Micro Computer, Inc.
All rights reserved.
Printed in the United States of America

Preface

About This Manual

This manual is written for system integrators, IT technicians and knowledgeable end-users. It provides instructions on how to install and configure the AOM-TPM-9655V/9655H on Supermicro motherboards.

Manual Organization

Chapter 1 provides an overview on the AOM-TPM-9655V/9655H.

Chapter 2 provides hardware installation, BIOS configuration, and the Intel Provision Utility setup instructions.

Conventions Used in This Manual

Pay special attention to the following symbols for proper installation and to prevent damage to the system or injury to yourself.

Warning: Important information given to ensure proper system installation or to prevent damage to the components or injury to yourself.

Note: Additional information given to ensure correct add-on module setup.

Contacting Supermicro

Headquarters

Address:	Super Micro Computer, Inc. 980 Rock Ave. San Jose, CA 95131 U.S.A.
Tel:	+1 (408) 503-8000
Fax:	+1 (408) 503-8008
Email:	marketing@supermicro.com (General Information) support@supermicro.com (Technical Support)
Web Site:	www.supermicro.com

Europe

Address:	Super Micro Computer B.V. Het Sterrenbeeld 28, 5215 ML 's-Hertogenbosch, The Netherlands
Tel:	+31 (0) 73-6400390
Fax:	+31 (0) 73-6416525
Email:	sales@supermicro.nl (General Information) support@supermicro.nl (Technical Support) rma@supermicro.nl (Customer Support)
Web Site:	www.supermicro.com

Asia-Pacific

Address:	Super Micro Computer, Inc. 3F, No. 150, Jian 1st Rd. Zhonghe Dist., New Taipei City 235 Taiwan (R.O.C)
Tel:	+886-(2) 8226-3990
Fax:	+886-(2) 8226-3992
Email:	support@supermicro.com.tw
Tel:	+886-(2)-8226-3990
Web Site:	www.supermicro.com.tw

Table of Contents

Preface

About This Manual 3

Manual Organization 3

Conventions Used in This Manual 3

Contacting Supermicro 4

Chapter 1 Overview

1-1 Overview of the AOM-TPM-9655V/9655H Card 1-1

1-2 Key Features 1-1

1-3 Specifications 1-2

Security Features 1-2

Application Support 1-2

Compliance/Environmental 1-3

Supported Platforms 1-3

Mechanical Specifications 1-3

Chapter 2 Installation and Configuration

2-1 The AOM-TPM-9655V/9965H Card 2-1

2-2 Add-on TPM Module Installation 2-2

2-3 Add-on TPM Module in UEFI BIOS 2-3

2-4 Intel Provision Utility 2-7

2-5 Add-On TPM Module in Legacy BIOS 2-13

Notes

Chapter 1

Overview

1-1 Overview of the AOM-TPM-9655V/9655H Card

The Supermicro add-on module AOM-TPM-9655V/9655H is a security device that stores RSA encryption keys specific to the host system for hardware authentication. The add-on module is based on Infineon's Trusted Platform Module (TPM), and its specifications are fully compliant and published by the Trusted Computing Group (TCG) certification process. The TPM is protected by an encapsulated microcontroller security chip to protect important information such as keys, passwords and digital ceritficates stored on the chip against external attacks and physical theft. The TPM module is paired with a motherboard and is integrated into the boot process to gather runtime information for trusted reporting.

The AOM-TPM-9655V/9655H is ideal for users looking for additional security for their systems.

1-2 Key Features

- TCG 1.2/2.0 compliant trusted platform module (TPM)
- Microcontroller in 0.22/0.09 um CMOS technology
- Compliant embedded software
- EEPROM for TCG firmware enhancements and for user data and keys
- Hardware accelerator for SHA-1 and SHA-256 hash algorithm
- True Random Number Generator (TRNG)
- Trick counter with tamper detection
- Protection against Dictionary Attack
- Infineon's TPM 1.2 is Common Criteria certified at Evaluation Assurance Level (EAL) 4 Moderate
- General Purpose Input/Output

- Intel® Trusted Execution Technology Support
- AMD® Secure Virtual Machine Architecture Support
- Full personalization with Endorsement Key (EK) and EK certificate
- Power saving sleep mode
- 3.3 V power supply
- WHQL dual mode 1.1b + 1.2 TPM Windows Kernel Mode Driver

1-3 Specifications

Security Features

- Over/Under voltage Detection
- Low frequency sensor
- High frequency filter
- Reset Filter
- Memory Encryption/Decryption (MED)

Application Support

- Microsoft Outlook® and Outlook Expres®
- Microsoft Office 2010, Office 2000, Office XP and Office 2003
- Microsoft Internet Explorer®
- Mozilla Firefox
- Mozilla Thunderbird
- Netscape Communicator®
- Microsoft Encrypted File System

- RSA Secure ID®
- Check Point SecuRemote/SecureClient
- Check Point VPN-1®/FireWall-1 NG®
- Entrust Desktop Manager Solutions
- Adobe Acrobat 6.0 Professional

Compliance/Environmental

- RoHS Compliant 6/6, Pb Free RoHS

Supported Platforms

- Supermicro motherboards with 20-pin TPM connectors

Mechanical Specifications

- Dimensions: 8mm x 26mm x 25mm (W x L x H) (AOM-TPM-9655V)
- Dimensions: 15.6mm x 26mm x 13.1mm (W x L x H) (AOM-TPM-9655H)

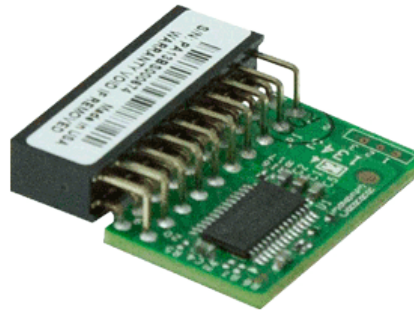
Notes

Chapter 2

Installation and Configuration

2-1 The AOM-TPM-9655V/9965H Card

The add-on module AOM-TPM-9655 comes in the vertical and horizontal forms. The AOM-TPM-9655V is the vertical and the AOM-TPM-9655H is the horizontal. See below for pictures of the add-on modules.



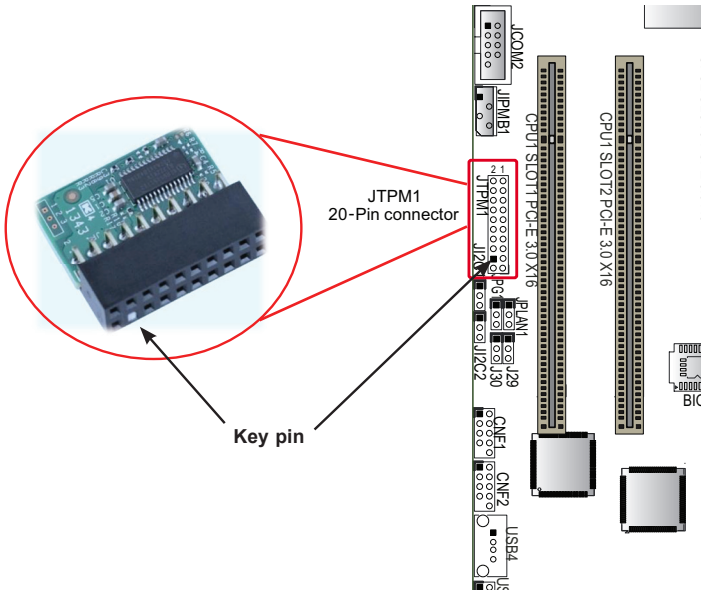
AOM-TPM-9655V

AOM-TPM-9655H

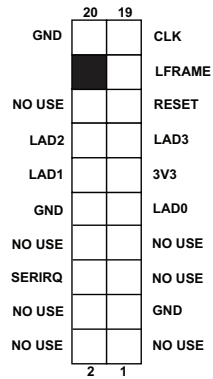
Note: For the add-on module support, an E5-2600 (C2 Stepping) CPU or later model is required.

2-2 Add-on TPM Module Installation

1. A 20-pin female connector is located on the AOM-TPM-9655V/9655H. When installing this add-on module to a motherboard, connect it to the 20-pin JTPM1 male connector on the Supermicro motherboard.



2. Pin 18 on the add-on module is the key pin. This key pin is a guide to help you install the add-on module in the right direction. See the image above for the key pin, and the image below for the pin definition.



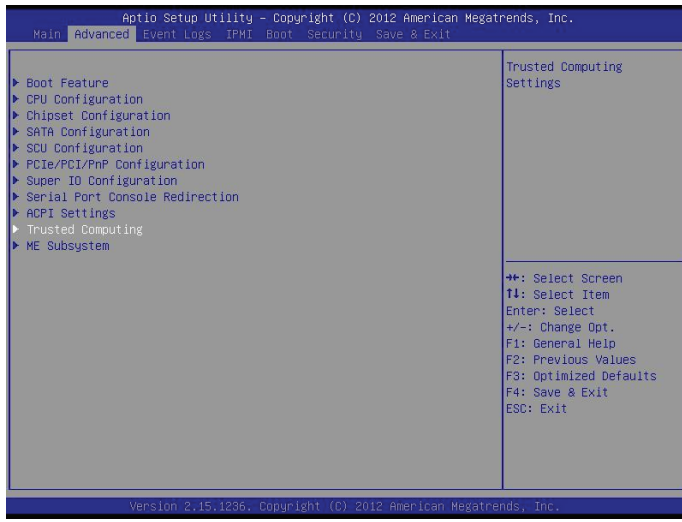
Note: Images displayed are for illustration only. The location of JTPM1 on your motherboard may differ from the illustration above.

2-3 Add-on TPM Module in UEFI BIOS

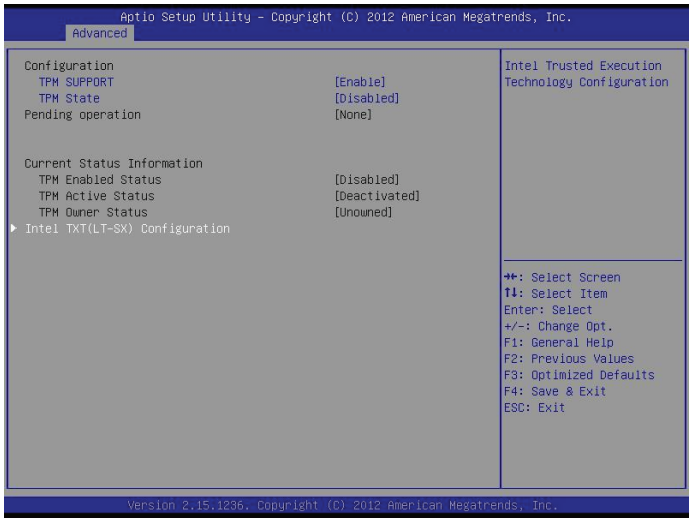
After you install the add-on TPM module on the motherboard, you need to configure the BIOS to detect the module.

1. On system boot-up, press the "DEL" key to enter the BIOS.

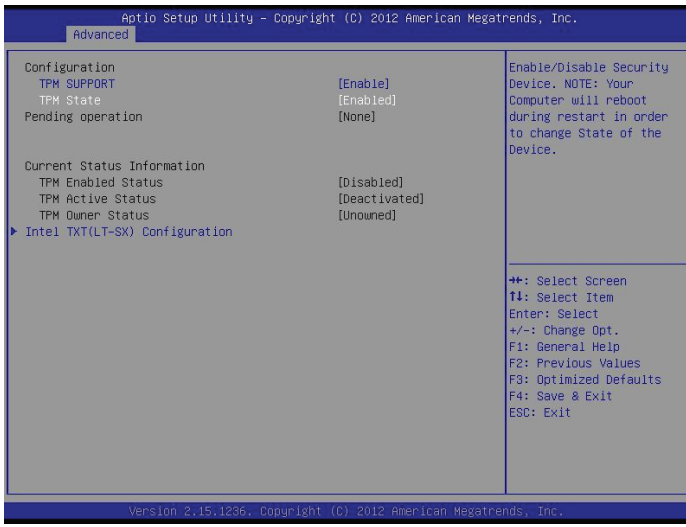
2. Once you are in the BIOS, you will start on the "Main" page. Press the right arrow key to move to the "Advanced" tab. If the add-on module is installed and detected by the system, "Trusted Computing" will appear.



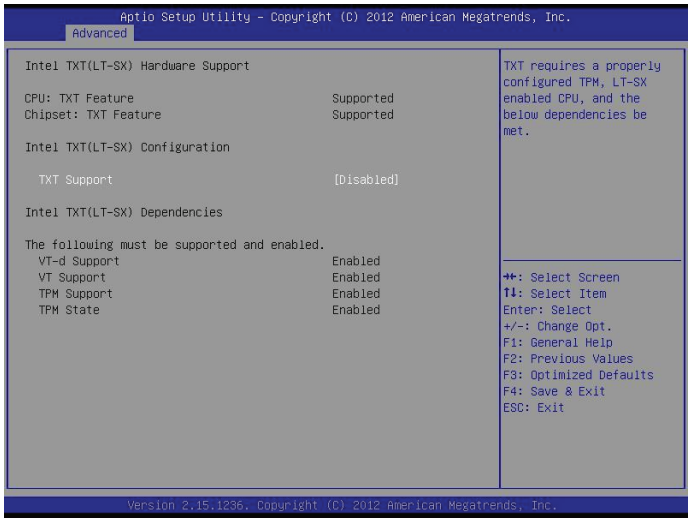
3. Select "Trusted Computing" and you will see the screen below.



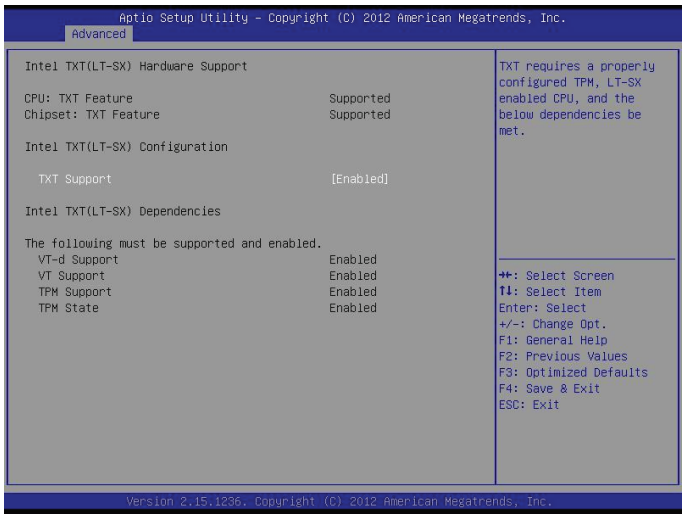
4. Change the "TPM State" feature to "Enabled."


Aptio Setup Utility – Copyright (C) 2012 American Megatrends, Inc.
Advanced
Configuration
TPM SUPPORT [Enable]
TPM State [Enabled]
Pending operation [None]
Current Status Information
TPM Enabled Status [Disabled]
TPM Active Status [Deactivated]
TPM Owner Status [Unowned]
Intel TXT(LT-SX) Configuration
Enable/Disable Security Device. NOTE: Your Computer will reboot during restart in order to change State of the Device.
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit
Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.

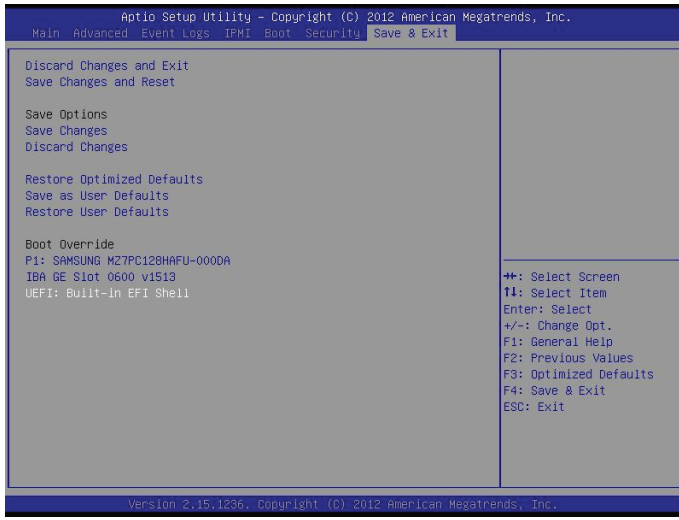
5. Scroll down and select "Intel TXT (LT-SX) Configuration."


Aptio Setup Utility – Copyright (C) 2012 American Megatrends, Inc.
Advanced
Intel TXT(LT-SX) Hardware Support
CPU: TXT Feature Supported
Chipset: TXT Feature Supported
Intel TXT(LT-SX) Configuration
TXT Support [Disabled]
Intel TXT(LT-SX) Dependencies
The following must be supported and enabled.
VT-d Support Enabled
VT Support Enabled
TPM Support Enabled
TPM State Enabled
TXT requires a properly configured TPM, LT-SX enabled CPU, and the below dependencies be met.
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit
Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.

6. Change the "TXT Support" feature to "Enabled."


Aptio Setup Utility – Copyright (C) 2012 American Megatrends, Inc.
Advanced
Intel TXT(LT-SX) Hardware Support
CPU: TXT Feature Supported
Chipset: TXT Feature Supported
Intel TXT(LT-SX) Configuration
TXT Support [Enabled]
Intel TXT(LT-SX) Dependencies
The following must be supported and enabled.
VT-d Support Enabled
VT Support Enabled
TPM Support Enabled
TPM State Enabled
TXT requires a properly configured TPM, LT-SX enabled CPU, and the below dependencies be met.
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit
Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.

7. Save and exit to complete the add-on TPM module BIOS configuration stage.



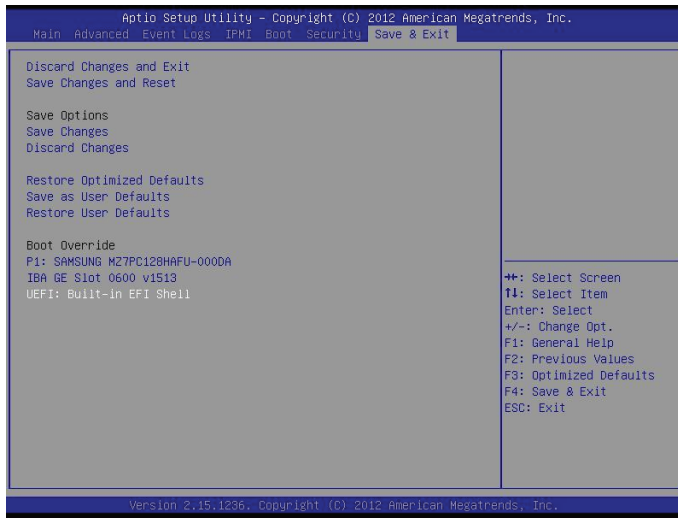
8. The next step is to run the Intel Provision Utility. Refer to the next section for instructions.

2-4 Intel Provision Utility

This section inlcudes instructions on how to run the Intel Provision Utility to lock the add-on TPM module. Contact Supermicro Technical Support to download a copy of the utility to a USB flash drive.

With the USB flash drive plugged into your system, you must boot to the EFI shell to run the utility. There are two ways you can boot to the EFI shell:

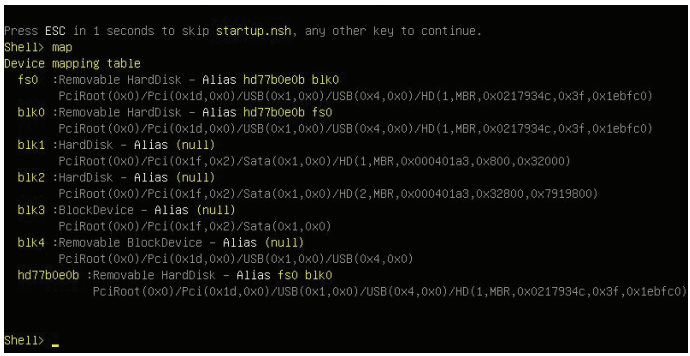
- **Option 1:** You can boot to the EFI shell from the "Save and Exit" screen of the BIOS. This is the same screen shown in Step 7 of Section 2-3. If you choose this option, select "UEFI: Built-in EFI Shell" and you will see the EFI shell (see the next page for the shell screen).



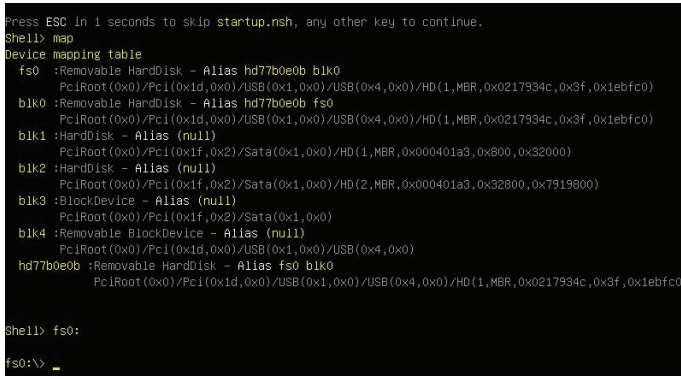
- **Option 2:** You can also boot to the EFI shell by pressing the "F11" key during system boot-up. If you choose this option, you will see the screen below:

Please select boot device:
P1: SAMSUNG MZ7PC128HAFU-000DA
Flash Drive UT_USB20 0.00
IBA GE Slot 0600 v1513
UEFI: Built-in EFI Shell
UEFI: Flash Drive UT_USB20 0.00
Enter Setup
↑ and ↓ to move selection
ENTER to select boot device
ESC to boot using defaults

1. Once you are at the utility shell screen, run the command: map
   This command displays a list of devices connected to the motherboard.

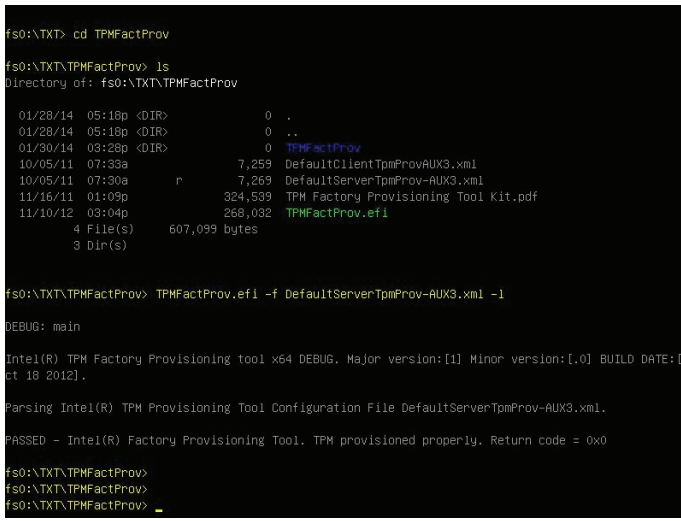


2. Then type "fs0:" This command takes you to the directory of the utility on the USB flash drive.



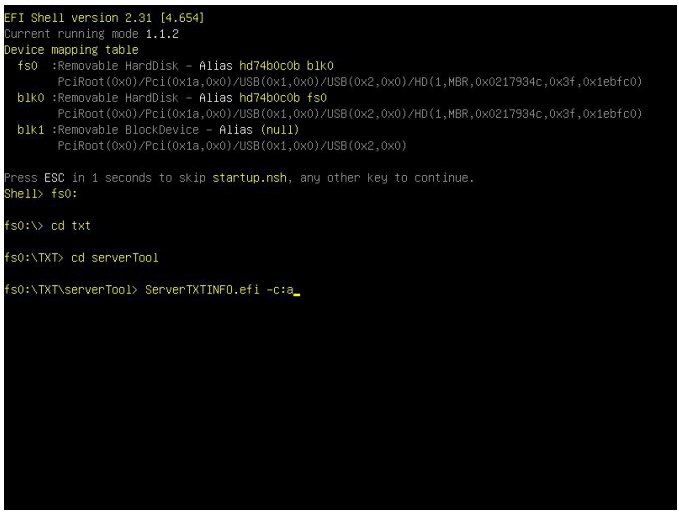
3. To lock the add-on TPM module, run the command:

TPMFactProv.efi –f DefaultServerTpmProv-AUX3.xml –l

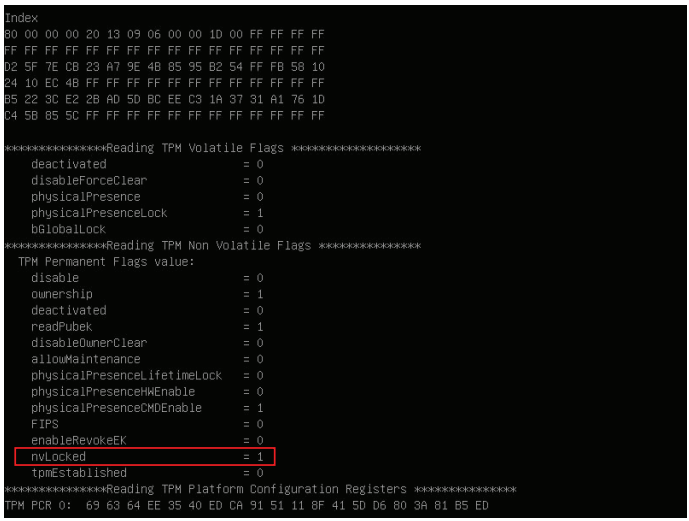

fs0:\TXT> cd TPMFactProv
fs0:\TXT\TPMFactProv> ls
Directory of: fs0:\TXT\TPMFactProv
01/28/14 05:18p <DIR> 0 .
01/28/14 05:18p <DIR> 0 ..
01/30/14 03:28p <DIR> 0 TPMFactProv
10/05/11 07:33a 7,259 DefaultClientTpmProvAUX3.xml
10/05/11 07:30a r 7,269 DefaultServerTpmProv-AUX3.xml
11/16/11 01:09p 324,539 TPM Factory Provisioning Tool Kit.pdf
11/10/12 03:04p 268,032 TPMFactProv.efi
4 File(s) 607,099 bytes
3 Dir(s)
fs0:\TXT\TPMFactProv> TPMFactProv.efi -f DefaultServerTpmProv-AUX3.xml -l
DEBUG: main
Intel(R) TPM Factory Provisioning tool x64 DEBUG. Major version:[1] Minor version:[.0] BUILD DATE:[O
ct 18 2012].
Parsing Intel(R) TPM Provisioning Tool Configuration File DefaultServerTpmProv-AUX3.xml.
PASSED - Intel(R) Factory Provisioning Tool. TPM provisioned properly. Return code = 0x0
fs0:\TXT\TPMFactProv>
fs0:\TXT\TPMFactProv>
fs0:\TXT\TPMFactProv>

4. To check if the add-on TPM is locked successfully, run the command:

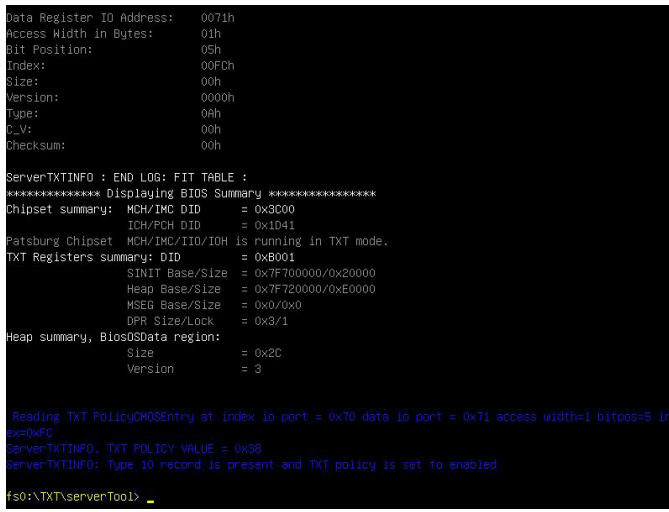
   ServerTXTINFO.efi -c:a


EFI Shell version 2.31 [4.654]
Current running mode 1.1.2
Device mapping table
fs0 :Removable HardDisk - Alias hd74b0c0b blk0
PciRoot(0x0)/Pci(0x1a,0x0)/USB(0x1,0x0)/USB(0x2,0x0)/HD(1,MBR,0x0217934c,0x3f,0x1ebfc0)
blk0 :Removable HardDisk - Alias hd74b0c0b fs0
PciRoot(0x0)/Pci(0x1a,0x0)/USB(0x1,0x0)/USB(0x2,0x0)/HD(1,MBR,0x0217934c,0x3f,0x1ebfc0)
blk1 :Removable BlockDevice - Alias (null)
PciRoot(0x0)/Pci(0x1a,0x0)/USB(0x1,0x0)/USB(0x2,0x0)
Press ESC in 1 seconds to skip startup.nsh, any other key to continue.
Shell> fs0:
fs0:\> cd txt
fs0:\TXT> cd serverTool
fs0:\TXT\serverTool> ServerTXTINFO.efi -c:a

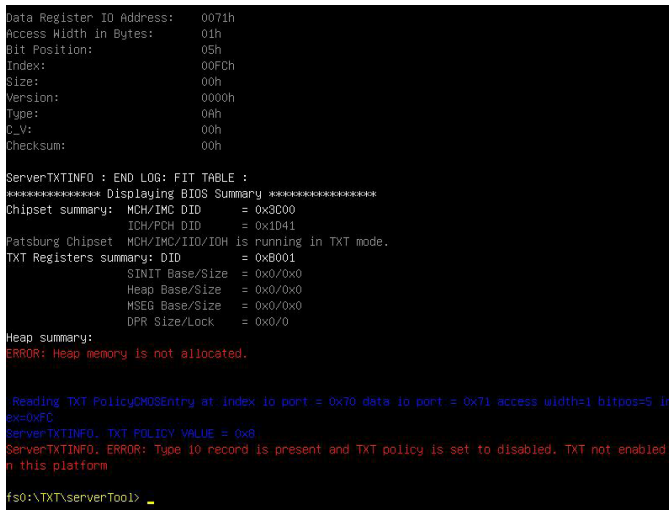
5. If the add-on TPM is successfully locked, the value of "nvLocked" equals 1. See the image on step 6 for the continuation of this screen.


Index
80 00 00 00 20 13 09 06 00 00 1D 00 FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
D2 5F 7E CB 23 A7 9E 4B 85 95 B2 54 FF FB 58 10
24 10 EC 4B FF FF FF FF FF FF FF FF FF FF FF FF
B5 22 3C E2 2B AD 5D BC EE C3 1A 37 31 A1 76 1D
C4 5B 85 5C FF FF FF FF FF FF FF FF FF FF FF FF
**********Reading TPM Volatile Flags **********
deactivated = 0
disableForceClear = 0
physicalPresence = 0
physicalPresenceLock = 1
bGlobalLock = 0
**********Reading TPM Non Volatile Flags **********
TPM Permanent Flags value:
disable = 0
ownership = 1
deactivated = 0
readPubek = 1
disableOwnerClear = 0
allowMaintenance = 0
physicalPresenceLifetimeLock = 0
physicalPresenceHWEnable = 0
physicalPresenceCMDEnable = 1
FIPS = 0
enableRevokeEK = 0
nvLocked = 1
tpmEstablished = 0
**********Reading TPM Platform Configuration Registers **********
TPM PCR 0: 69 63 64 EE 35 40 ED CA 91 51 11 8F 41 5D D6 80 3A 81 B5 ED

6. The screen below is a continuation of the screen on step 5.


Data Register IO Address: 0071h
Access Width in Bytes: 01h
Bit Position: 05h
Index: 00FCh
Size: 00h
Version: 0000h
Type: 0Ah
C_V: 00h
Checksum: 00h
ServerTXTINFO : END LOG: FIT TABLE :
********** Displaying BIOS Summary **********
Chipset summary: MCH/IMC DID = 0x3C00
ICH/PCH DID = 0x1D41
Patsburg Chipset MCH/IMC/IIO/IOH is running in TXT mode.
TXT Registers summary: DID = 0xB001
SINIT Base/Size = 0x7F700000/0x20000
Heap Base/Size = 0x7F720000/0xE0000
MSEG Base/Size = 0x0/0x0
DPR Size/Lock = 0x3/1
Heap summary, BiosOSData region:
Size = 0x2C
Version = 3
Reading TXT PolicyCMOSEntry at index io port = 0x70 data io port = 0x71 access width=1 bitpos=5 ind
ex=0xFC
ServerTXTINFO. TXT POLICY VALUE = 0x38
ServerTXTINFO: Type 10 record is present and TXT policy is set to enabled
fs0:\TXT\serverTool>

7. If the description and value show up in red, then the lock was unsuccessful. See the error messages in red in the image below.


Data Register IO Address: 0071h
Access Width in Bytes: 01h
Bit Position: 05h
Index: 00FCh
Size: 00h
Version: 0000h
Type: 0Ah
C_V: 00h
Checksum: 00h
ServerTXTINFO : END LOG: FIT TABLE :
********** Displaying BIOS Summary **********
Chipset summary: MCH/IMC DID = 0x3C00
ICH/PCH DID = 0x1D41
Patsburg Chipset MCH/IMC/IIO/IOH is running in TXT mode.
TXT Registers summary: DID = 0xB001
SINIT Base/Size = 0x0/0x0
Heap Base/Size = 0x0/0x0
MSEG Base/Size = 0x0/0x0
DPR Size/Lock = 0x0/0
Heap summary:
ERROR: Heap memory is not allocated.
Reading TXT PolicyCMOSEntry at index io port = 0x70 data io port = 0x71 access width=1 bitpos=5 ind
ex=0xFC
ServerTXTINFO. TXT POLICY VALUE = 0x8
ServerTXTINFO. ERROR: Type 10 record is present and TXT policy is set to disabled. TXT not enabled o
n this platform
fs0:\TXT\serverTool>

8. If the add-on TPM lock was unsuccessful and you received an error message, follow the steps below to troubleshoot the problem:

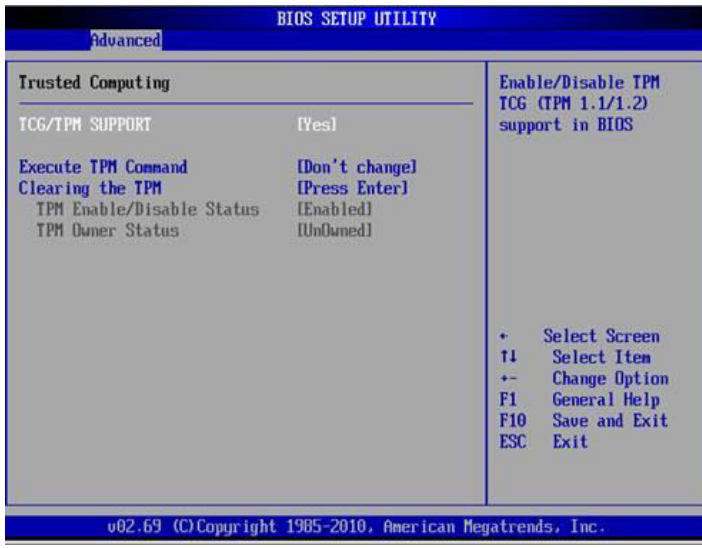
- Make sure that you are using a supported CPU (E5-2600 C2 Stepping or later model).
- Go to the "Advanced" tab of the BIOS and make sure "TXT Support" is enabled.
- Check the add-on TPM card if it is installed properly on the motherboard.
- Contact Supermicro Technical Support for additional assistance.

2-5 Add-On TPM Module in Legacy BIOS

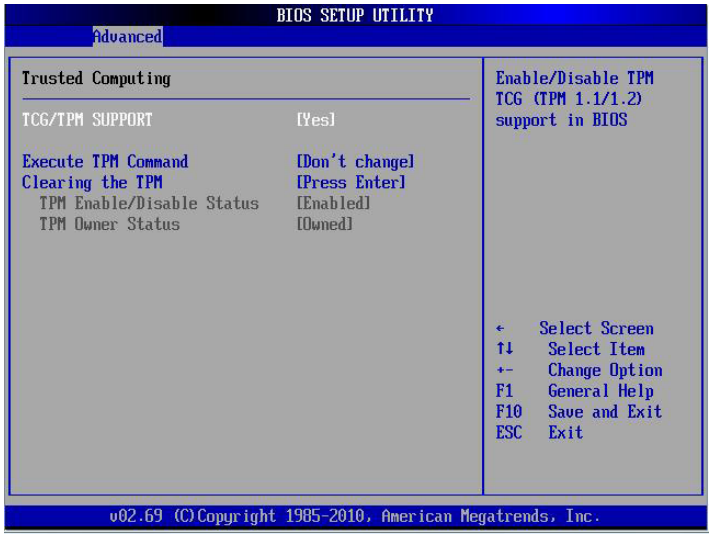
This section inlcudes instructions on how to run the add-on TPM module Legacy BIOS configuration to lock (Owned) the module in the Windows 7 operating system.

Note: Legacy BIOS is for AMD systems.

1. In the "Advanced" tab of the BIOS, enable "TPM Support" by selecting "Yes."



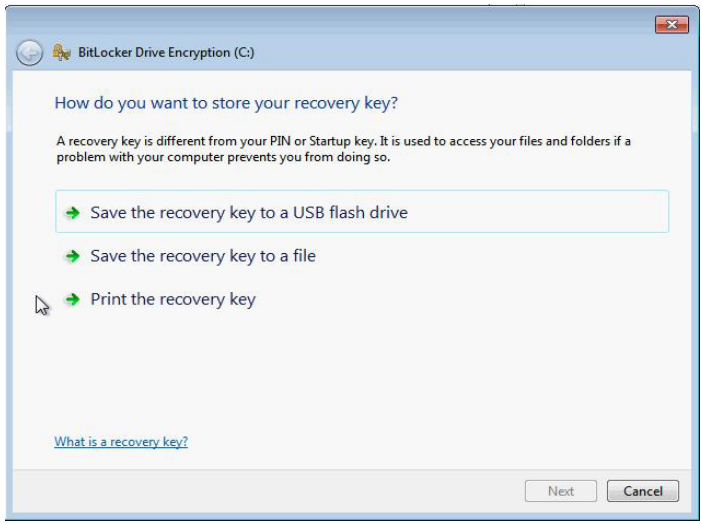
2. Highlight "Clearing the TPM" and hit Enter. Then the system will automatically reboot for the changes to take effect. After the system reboot, go back to the "Advanced" tab of the BIOS for the next step.



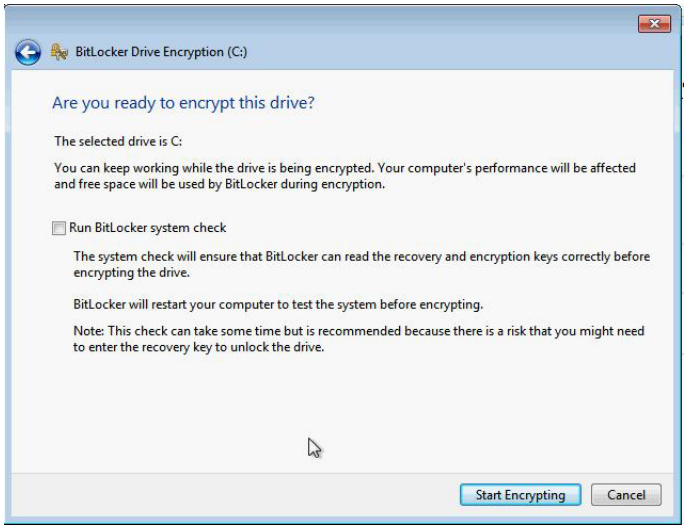
3. In the "Advanced" tab, highlight "Execute TPM Command" and select "Enabled." Exit the BIOS and boot to Windows 7.

4. Once you are in Windows 7, open the Control Panel and select "BitLocker Drive Encryption." to turn on the BiteLocker.

5. You will be given options on how you want to store the recovery key. In the screen below, select "Save the recovery key to a file" and save it on a USB flash drive.


BitLocker Drive Encryption (C:)
How do you want to store your recovery key?
A recovery key is different from your PIN or Startup key. It is used to access your files and folders if a problem with your computer prevents you from doing so.
Save the recovery key to a USB flash drive
Save the recovery key to a file
Print the recovery key
What is a recovery key?
Next
Cancel

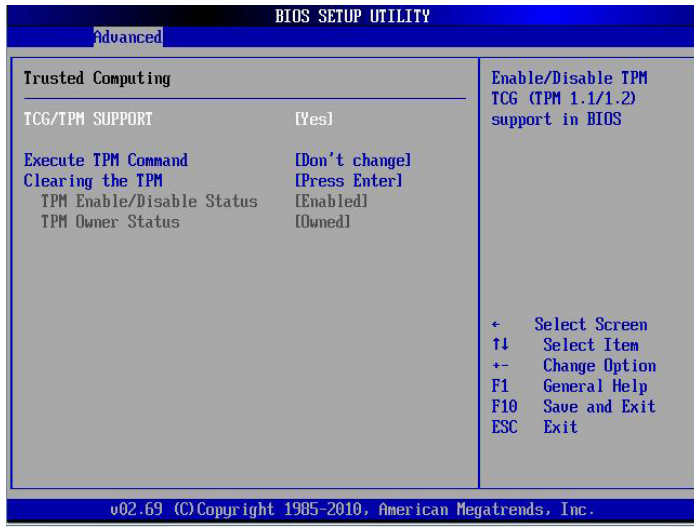
6. After you save the TPM recovery key on a USB flash drive, the encryption of drive C: will begin. Select "Start Encryption" to start the encryption.


BitLocker Drive Encryption (C:)
Are you ready to encrypt this drive?
The selected drive is C:
You can keep working while the drive is being encrypted. Your computer's performance will be affected and free space will be used by BitLocker during encryption.
Run BitLocker system check
The system check will ensure that BitLocker can read the recovery and encryption keys correctly before encrypting the drive.
BitLocker will restart your computer to test the system before encrypting.
Note: This check can take some time but is recommended because there is a risk that you might need to enter the recovery key to unlock the drive.
Start Encrypting
Cancel

7. After the encryption is complete, go to the Control Panel to check the status of BitLocker. You should see three options: **Turn Off BitLocker**, **Suspend Protection**, **Manage BitLocker.**

Help protect your files and folders by encrypting your drives
BitLocker Drive Encryption helps prevent unauthorized access to any files stored on the drives shown below. You are able to use the computer normally, but unauthorized users cannot read or use your files.
What should I know about BitLocker Drive Encryption before I turn it on?
BitLocker Drive Encryption - Hard Disk Drives
C:
On
Turn Off BitLocker
Suspend Protection
Manage BitLocker

8. You can also check the status in the BIOS. If the TPM module is locked, the "TPM Owner Status" should indicate "Owned."



Notes

(Disclaimer Continued)

The products sold by Supermicro are not intended for and will not be used in life support systems, medical equipment, nuclear facilities or systems, aircraft, aircraft devices, aircraft/emergency communication devices or other critical systems whose failure to perform be reasonably expected to result in significant injury or loss of life or catastrophic property damage. Accordingly, Supermicro disclaims any and all liability, and should buyer use or sell such products for use in such ultra-hazardous applications, it does so entirely at its own risk. Furthermore, buyer agrees to fully indemnify, defend and hold Supermicro harmless for and against any and all claims, demands, actions, litigation, and proceedings of any kind arising out of or related to such ultra-hazardous use or sale.